PD IEC TR 63201:2019

BSI Standards Publication

Low-voltage switchgear and controlgear – Guidance for the development of embedded software

bsi.

National foreword

This Published Document is the UK implementation of IEC TR 63201:2019.

The UK participation in its preparation was entrusted to Technical Committee PEL/121/1, Low voltage switchgear and controlgear.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2019

ISBN 978 0 539 01117 3

ICS 29.130.20

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 June 2019.

Amendments/corrigenda issued since publication

Date	Text affected

IEC TR 63201

Edition 1.0 2019-05

TECHNICAL REPORT

colour inside

Low-voltage switchgear and controlgear – Guidance for the development of embedded software

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 29.130.20

ISBN 978-2-8322-7006-6

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Terms and definitions 7
4 Risk assessment and identification of the main functions 10
5 Design management 10
5.1 Objective 10
5.2 Software management plan of the main functions 10
5.3 Configuration management 11
5.4 Change management 11
5.5 Defect management 12
5.6 System build and release processes 13
5.6.1 Binary generation 13
5.6.2 Release management 13
6 Manual parameterization of the embedded software 13
6.1 General 13
6.2 Influences on main function related parameters 14
6.3 Requirements for software-based manual parameterization 14
6.4 Verification of the parameterization tool 15
6.5 Documentation of software-based manual parameterization 15
7 Design lifecycle 15
7.1 General 15
7.2 Tools usage 16
7.3 Software lifecycle 16
7.3.1 Software lifecycle model 16
7.3.2 Independence of review, testing and verification activities 17
7.4 Requirements definition 18
7.4.1 General 18
7.4.2 System requirements 18
7.4.3 Software requirements specification 18
7.5 Software architecture 20
7.5.1 General 20
7.5.2 Software architecture specification 20
7.6 Software unit design 20
7.6.1 General 20
7.6.2 Input information 20
7.6.3 Software unit specification 21
7.7 Coding 21
7.8 Software unit test 22
7.9 Software integration test 22
7.10 Software testing 22
7.10.1 General 22
7.10.2 Test planning and execution 23

7.11 Documentation 23
7.12 Configuration and change management process 24
7.13 Verification and relationship with the validation of the equipment or system 24
Bibliography 26

Figure 1 – Defect management process 12
Figure 2 – V-model of software lifecycle 17

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR – GUIDANCE FOR THE DEVELOPMENT OF EMBEDDED SOFTWARE

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 63201, which is a technical report, has been prepared by subcommittee 121A: Low-voltage switchgear and controlgear, of IEC technical committee 121: Switchgear and controlgear and their assemblies for low voltage.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
121A/256/DTR	121A/287A/RVDTR

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Programmable electronics are now being integrated within switchgear and controlgear. For example, soft-starters, electronic overload relays, circuit-breakers with electronic trip units, proximity switches with built in micro-controllers and some accessories such as extension modules and control panels are using programmable electronics with embedded software called firmware. This embedded software often supports the main functions (see 3.3) provided by the equipment such as overcurrent protection and other important functions, e.g. alarm detection from monitoring devices.

The integration of embedded software within switchgear and controlgear should not degrade the integrity of their main functions compared to purely electromechanical equipment. Therefore, a minimum set of standard requirements for embedded software is provided by this document.

This document takes into account the existing best practices for developing embedded software within safety functions for automation given by IEC 61508-3. Functional safety approach is mainly used in machinery, automotive, automation and process automation where safety functions are implemented with multiple components which should match a consistent level of integrity when combined. In other sectors, such as electric distribution and power control systems, key functions such as over-current release, residual current release, load monitoring, etc. should follow installation rules and coordination rules which are systematically safety and reliability related. Therefore, this document can be seen as providing the principles of the good practice given by IEC 61508-3.

This document is also intended to provide an up-to-date method with regards to the supplement SE of UL 489.

The intention of this document is to provide guidance about:

– risk assessment aspects in relation to embedded software;
– embedded software evaluation method;
– software architecture;
– basic coding rules;
– measures to control software errors;
– software verification and its relationship with the validation of the equipment or system.

In this document, the term "software" is used as a generalized term for embedded software.

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR – GUIDANCE FOR THE DEVELOPMENT OF EMBEDDED SOFTWARE

1 Scope

This document provides information, and recommended minimum requirements related to embedded software supporting the main functions of switchgear and controlgear during the whole lifecycle of the equipment. It includes also the parameterization aspects and basics about secure coding standards.

This document can be used in addition to product standard requirements when not already covered.

This document is appropriate for new development or major changes in existing equipment.

This document is not intended to cover the functional safety of control systems for machinery or for automation which are covered by IEC 62061, ISO 13849-1 and IEC 61508 (all parts), neither the cybersecurity risk which are covered by ISO 27005, and IEC 62443 (all parts). It gives only some example of secure coding rules.

NOTE Future new publication IEC TS 63208[1] is under development for implementing embedded cybersecurity measures within switchgear and controlgear based on ISO 27005 and IEC 62443 (all parts).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-1:1993, as well as the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
embedded software
software, supplied by the manufacturer, that is an integral part of the equipment and that is not accessible for partial modification

Note 1 to entry: Firmware and system software are examples of embedded software.

Note 2 to entry: An embedded software can be upgraded by an integral upload.

[1] Future publication IEC TS 63208 is currently at CD stage.